An Enterprise Backup Solution for GOES Operations Ground Equipment (OGE) and Spacecraft Support Ground System (SSGS)

Abhishek Agarwal[1], Rachid Dahmani[1], Shahram Tehranian[1], Keith McKenzie[2]

[1]Avaya Government Solutions
[2]National Environmental Satellite, Data, and Information Service (NESDIS)

Abstract – NOAA's National Environmental Satellite, Data, and Information Service (NESDIS) provides timely access to global environmental data from satellites and other sources to promote, protect, and enhance the Nation's economy, security, environment, and quality of life. The Office of Systems Development (OSD) Ground Systems Division (GSD) intends to provide an enterprise-wide backup system for all GOES I-M and GOES NOP Operations Ground Equipment (OGE) and Spacecraft Support Ground System (SSGS) components. The components that constitute the OGE and SSGS include the Sensor Processing System (SPS), Replacement Product Monitor (RPM), Consolidated Analysis Workstations (CAWS), Orbit and Attitude Tracking System (OATS), SPS Database Servers, Domain Controllers, GOES NOP Telemetry and Command System (GTACS), GOES NOP Telemetry Acquisition and Command Transmission System (NTACTS), and Multi-use Data Link (MDL) Receive System and Server (MRS&S).

The objective of the GOES Backup System (GBS) is to provide a backup and restore capability of individual files, and to provide Disaster Recovery (DR) including bare metal recovery of GOES ground system components. The GBS is developed to protect NOAA critical assets with the ability to back up, restore, and recover mission-critical data associated with operational GOES ground system components. The GBS provides the capability for system administrators to schedule automated system backup from a centralized location. System administrators will be able to perform remote backup and restore of data for all operational ground system components; execute pre-determined automated backup of complete systems, data and applications; perform short-term online data backups using a Storage Area Network (SAN) followed by offline data migration to tapes for long-term archival; and conduct simultaneous backup and restore operations from multiple servers using online backup.

This paper describes the design, development, testing, and deployment of an enterprise backup solution to provide backup and recovery of GOES ground system components at Wallops/Fairbanks Command and Data Acquisition Station (WCDAS/FCDAS), Wallops Backup Unit (WBU), and NOAA Satellite Operations Facility (NSOF). GBS units have been deployed at the aforementioned NOAA facilities and are in the process of transitioning to operation.

Index Terms – GOES, Ground System Data Processing, Blades, Data Backup and Disaster Recovery, Continuity of Operations (COOP), GOES Enterprise Managed System (GEMS)

I. INTRODUCTION

In an effort to upgrade the GOES Operations Ground Equipment (OGE) and Spacecraft Support Ground System (SSGS) hardware components to more centralized low maintenance architecture with reliable short and long term data backup and recovery, the GOES Enterprise Managed System (GEMS) architecture was developed. This architecture makes it possible to install the hardware in a single compact rack where electronic components, network devices, power, and cooling can be shared. This provides a unified and efficient architecture and allows for future expansion.

Two main OGE components, the Replacement Product Monitor (RPM) and the Sensor processing System (SPS) have already been migrated to the GEMS architecture utilizing server blades with Opteron processors running the Solaris-10 operating system. This architecture consolidates several servers in one blade enclosure with centralized management and monitoring. It also has built-in redundancy for various components such as disks, power supplies, and cooling fans to ensure uninterrupted operation and low maintenance costs.

To protect OGE components against system failure and ensure uninterrupted operation, a GOES Backup System (GBS) was developed and integrated into the GEMS architecture. It is a fully managed and scalable system implemented as part of GEMS (Reference 1). GBS can be used to manually or automatically, on a regular schedule, backup all data, such as the operating system (OS), system configuration files, system images, database files, and other system specific files on any of the OGE and SSGS ground system components. The main functions of the GBS include:

- Perform remote backup and restore of data on OGE and SSGS components;
- Provide capability to simultaneously backup and restore multiple servers using online backup;
- Support offline data transfer to tapes for long-term backup storage;
- Provide short-term data backups on a Storage Area Network (SAN) to facilitate faster data retrieval;
- Run pre-determined automated backup of complete system, data and applications as needed;
- Support selective restore of data as needed;
- Perform backup using back-end Fibre Channel connection from backup server to SAN to minimize network loading;
- Fulfill NOAA IT security and Continuity of Operations (COOP) requirements;
- Provide a scalable and adaptable solution allowing for future growth and expandability.

The GBS system is currently deployed at WCDAS and NSOF where it is installed on the GEMS RPM racks (Reference 2) and at WBU and FCDAS as standalone systems. At each site it provides data protection for a variety of platforms, including Unix, Linux and Windows operating systems. The user can perform manual backups or set up periodic calendar-based backup schedules to perform automatic, unattended backups for any client on the GOES network. During a backup, the client sends backup data across the network to the backup server, which performs the type of storage that is specified in a preset backup policy. During a restore, users can browse the desired backup data that is available and select the files and directories to recover.

The purpose of the GBS is to provide a centrally managed, network-based mechanism for protecting GOES ground system components against interruption of operations or lengthy downtimes, and provide fast recovery in case of system failure. Client machines are protected when added to a backup protection policy that is used to regularly perform backups on a predetermined schedule. The backup policy can specify the type of data, files and directories, a specific schedule for each client or group of clients, and the location to store the backup data. In addition, the backups include all the information, including operating systems, data files, and configuration and system files, that are required to recover a system from a total system failure.

II. SYSTEM ARCHITECTURE AND DESIGN

Hardware Architecture

The GBS was developed in the GEMS architecture environment where server blades based on x86 Opteron processors were used (Reference 3). This architecture consolidates the hardware in a single compact blade enclosure (Reference 4) where electronic components, power, and cooling can be shared. This provides a unified and efficient centralized management using an onboard administrator (Reference 5) that is installed within the enclosure. It also has built-in redundancy for various components such as disks, power supplies, and cooling fans to ensure uninterrupted operation and low maintenance costs. Several server blades can be installed in one blade enclosure and share all the resources available within the enclosure.

The main hardware components of the GBS are the backup and installation servers. The hardware architecture of the GBS systems at WCDAS and NSOF consists of two clustered HP server blades running Microsoft Windows Server 2008 Enterprise operating system. In addition to Ethernet connections, each server will connect to the Storage Area Network (SAN) via redundant Fibre Channel switches. Two Tape Libraries are also connected to the Fibre Channel switches. The two clustered servers are used as Cell Manager for the GBS and as Installation Server for all Windows platforms. A Red Hat Linux server is used for the installation of GBS client software on all Unix and Linux clients.

Figure 1 shows the GBS hardware architecture at WCDAS and NSOF. The main hardware components are:

- Two backup server blades configured in a clustered environment to improve performance and connectivity, and eliminate single points of failure. The clustered servers are also used as installation servers for Windows clients;
- One Unix installation server for Unix, Linux, Solaris, and AIX machines;
- Two Cisco Ethernet switches to provide redundant Ethernet connectivity;
- Two Fibre Channel switches to provide redundant Fibre Channel connectivity;
- Two tape libraries for long-term backup and restore;
- Two SAN disk shelves each with12x1TB FATA drives;
- Redundant SAN controllers, power supplies, cooling fans, and power distribution units.

The hardware is configured with built-in redundancy to protect data and network connectivity in case of hardware failure of individual GBS hardware components. This protection includes:

- Redundant Fibre Channel connectivity to SAN and tape library;
- Redundant Ethernet connectivity for network backup;
- End-to-end Fibre Channel connectivity from server to storage;
- RAID-5 hard disk configuration.

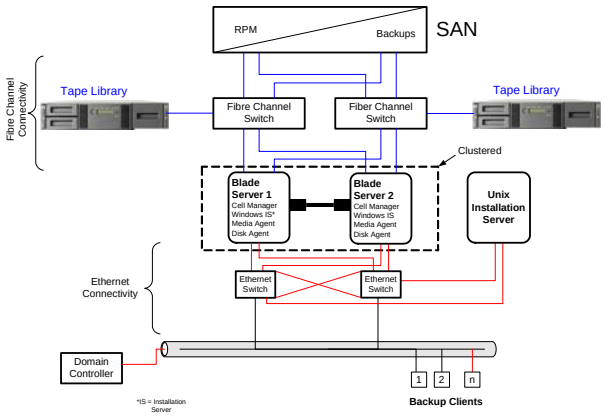

Figure 1. GBS Hardware Configuration at WCDAS and NSOF.

A scaled down version of GBS is installed at WBU and FCDAS. It includes a standalone backup server running Microsoft Windows Server 2008 Standard operating system. It serves as the Cell Manager for the GBS and as Installation Server for all Windows platforms. A separate Red Hat Linux standalone server is used for the installation of GBS client software on all Unix and Linux clients. Figure 2 shows the hardware architecture for the GBS installed at WBU and FCDAS.

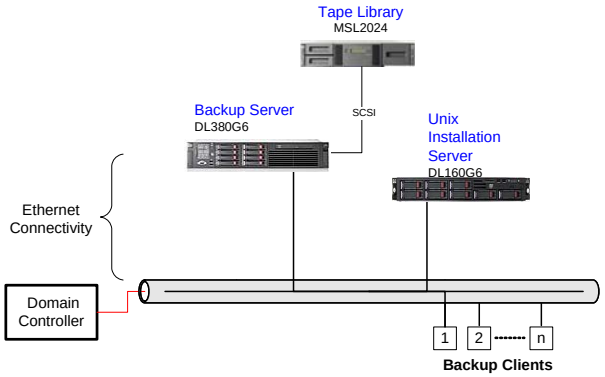

Figure 2. GBS Hardware Configuration at WBU and FCDAS.

Software Architecture

The GBS software architecture is based on HP Data Protector software (Reference 6). It provides protection of data, applications, and operating system on a single machine or a large network of machines. This simple and reliable data protection can be used for Windows, Linux, and other types of Unix platforms, with the ability to backup to disk, tape, or DVD/CD. Additional backup clients can be added as needed, and all backups are managed from a single interface. The following are short descriptions of the main components of HP Data Protector software.

Cell Manager: Functions as the central point of communication and tasking in the HP Data Protector environment. All OGE and SSGS components included in the backup system (cell network) report to the Cell Manager, which controls all backup and restore sessions with all clients within the cell. The cell manager also maintains an Internal Database (IDB) where all aspects of the backup process are stored. Information such as backup durations, media identification, session identification, client information and licensing are maintained in the IDB.

Disk Agent: Functions as the backup agent and is the required client software for basic backup operation on all computer platforms. An instance of this software will be installed on all OGE and SSGS components requiring backup, restore, and recovery. The Disk Agent supports both Windows and Unix operating systems.

Media Agent: Resides on the Backup Server and is connected to backup devices such as tape libraries or Storage Area Networks (SAN). The Media Agent software is installed on the clustered backup server that is attached to the SAN and the tape library.

Installation Server: Holds a repository of the HP Data Protector Client software packages such as Media Agent, Disk Agent, Application Agent, etc., for a specific architecture (i.e. Unix, HPUX, Red Hat Linux, Solaris, and Windows). By default, the Installation Server resides on the same machine as the Cell Manager. At least two Installation Servers are needed where both Windows and Unix/Linux operating systems are used. In the GBS environment, the Windows Installation Server resides on the Cell Manager while the Unix Installation Server resides on a separate Red Hat Linux Server.

The Cell Manager is used to administer all backup functions on the servers and all other clients that have the HP Data Protector Client software installed and configured. It also manages the storage devices (SAN and Tape Library), and stores and manages backup policies and schedules. Backup and restore functions are performed remotely from the Backup Server. Two Windows 2008 Server Standard/Enterprise backup servers are configured in a Windows clustered environment to provide backup server redundancy and fast network connection, improve performance, and to eliminate single points of failure. The backup software runs as a single clustered application.

GBS can be used for backup and restore operations on clients running on Unix, Linux, and Windows operating systems. The main software components of the GBS are:

- Cell Manager;
- Installation server for Windows clients;
- Installation server for Unix/Linux clients;
- Storage Area Network (SAN) for short-term storage of backup files and directories;
- Tape Library for long-term storage of backup data;

Figure 3 and Figure 4 show the GBS software components and the path for data backup on the GBS at WCDAS/NSOF and WBU/FCDAS, respectively. On

the systems at WCDAS and NSOF, data is first backed up online on the SAN for short-term storage and then transferred offline to the tape libraries, whereas on the systems at WBU and FCDAS data is first backed up online on the Cell Manager for short-term storage and then transferred offline to the tape library.

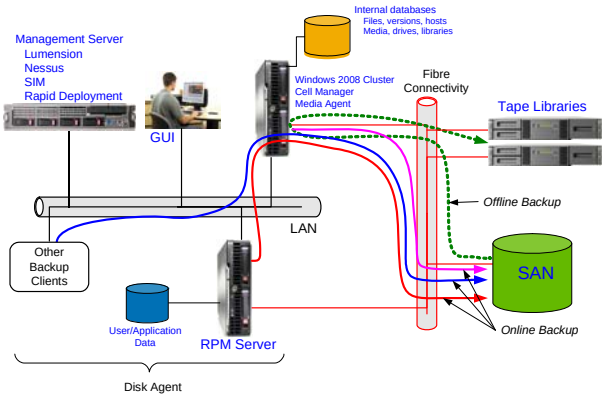

Figure 3. GBS Software Configuration at WCDAS and NSOF.

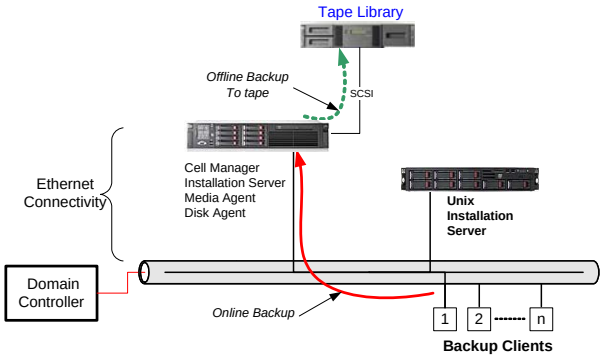

Figure 4. GBS Software Configuration at WBU and FCDAS.

III. IMPLEMENTATION

The GBS system was installed at WCDAS and NSOF in the blade enclosure on the GEMS RPM racks. It shares all network, monitoring, and management resources with the RPM servers. The three GBS servers (two clustered server blades for the Cell Manager and one server blade for the Unix installation server) are installed next to the RPM server blades. The GBS at WBU and FCDAS are installed on existing racks as standalone equipment. The GBS system rack configuration at WCDAS and NSOF is shown in Figure 5.

Setting up the GBS involves the installation of the servers on the rack followed by the installation and configuration of the software. The installation and configuration of HP Data Protector software involves the following main steps:

- Setting up a Windows server 2008 cluster;
- Installing HP Data Protector Software on the Windows Server 2008 cluster;
- Installing a Unix Installation Server;
- Importing the Unix Installation Server to the Cell Manager;
- Installing HP Data Protector Client Software on Windows clients;
- Installing HP Data Protector Client Software on Unix/Linux clients;
- Configuring clients in the Cell Manager;
- Creating backup policies.

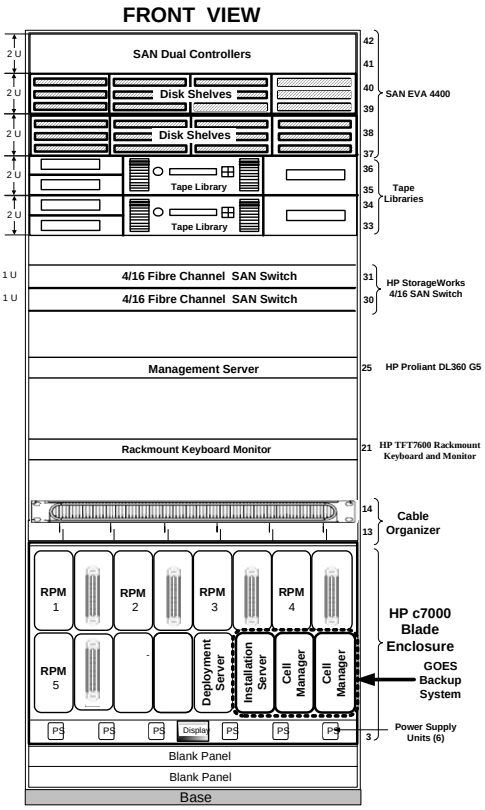

Figure 5. GBS Rack Configuration at WCDAS and NSOF.

After hardware installation and software configuration, the GBS system was fully tested and integrated into the GOES ground system infrastructure. It was successfully used to perform a full backup and restore of GOES servers while in normal operation. System resources on the servers were monitored throughout the backup and restore processes. These resources were only minimally affected by the GBS and were always available for use by the applications running on the servers. In addition, during the backup, network ports were monitored to measure the amount of incoming and outgoing data to determine the load on the network. The backup and restore processes had no adverse effect on the normal operations of the OGE and SSGS servers.

IV. CONCLUSION AND FUTURE WORK

A backup system for the GOES ground systems components has been successfully developed, tested, and deployed at four different NOAA locations including WCDAS, NSOF, WBU, and FCDAS. It is used for backing up and restoring application data, configuration files, system files, and operating system on selected servers and workstations that make up the GOES OGE and SSGS. The GBS can be extended in the future with an increase in its backup capacity by adding more tape libraries and disks shelves on the SAN. In addition, more system components can be protected by adding them to the backup system environment.

REFERENCES

[1] Tehranian S., Agarwal A., Vasanth S., Dahmani R., DiRosario R., Zang H., Madani H., Minus H., McKenzie K., Yu P., "GOES Enterprise Managed System (GEMS), Re-Architecting GOES Operations Ground Equipment (OGE), 89th AMS Annual Conference, January 2009.

[2] GOES Enterprise Managed System (GEMS) Hardware operation and Maintenance Manual, Revision 0, July 2010.

[3] AMD Opteron Processors, Retrieved (12/31/08) from http://h18004.www1.hp.com/products/servers/proliant-bl/c-class/465c-g5/index.html

[4] HP BladeSystem c7000 Enclosure Overview, Retrieved (12/31/08) from http://h18004.www1.hp.com/products/blades/components/enclosures/c-class/c7000/

[5] HP BladeSystem Onboard Administrator User Guide, Retrieved (12/31/08) from http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00705292/c00705292.pdf

[6] HP Data Storage Data Protector Software, Retrieved (12/31/08) from http://h18006.www1.hp.com/products/software/im/biz_continuity_avail/dp/index.html